

**UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION**

SCHNUCK MARKETS, INC.,

Plaintiff,

V.

FIRST DATA MERCHANT DATA
SERVICES CORP., and
CITICORP PAYMENT SERVICES, INC.,

Defendants.

Case No. 4:13-CV-2226-JAR

The Honorable John A. Ross

DEFENDANTS FIRST DATA
MERCHANT SERVICES CORP. AND CITICORP PAYMENT
SERVICES, INC.'S MOTION FOR JUDGMENT ON THE PLEADINGS

Defendants/Counterclaim-Plaintiffs First Data Merchant Services Corp. (“First Data”) and Citicorp Payment Services, Inc. (“Citicorp”) (collectively, the “Defendants”), by and through their counsel of record, move this Court pursuant to Federal Rule of Civil Procedure 12(c) for judgment on the pleadings with respect to Plaintiff/Counterclaim-Defendant Schnuck Markets, Inc.’s (“Schnucks” or “Plaintiff”) Complaint and Defendants’ Counterclaim. In support of the Motion, Defendants state as follows:

1. On November 4, 2013, Plaintiff initiated this action by filing the Complaint (Doc. #9) asserting causes of action for Breach of Contract and Declaratory Judgment.

2. The allegations of the Complaint arise out of a March 2013 cyber-attack sustained by Schnucks that resulted in a data breach adversely impacting its credit and debit card using customers. Schnucks commenced these proceedings in an effort to avoid its clear financial responsibility for the consequences of its data breach.

3. Specifically, Plaintiff claims that its financial responsibility is contractually limited to \$500,000. However, a plain language reading of the contractual provision relied on by Plaintiff demonstrates that this limitation does not apply here. Plaintiff is exclusively liable for 100% of the financial responsibility imposed by the card brand associations Visa and MasterCard (collectively the “Associations”) for the data breach.

4. On January 21, 2014, Defendants filed their Answer, Affirmative Defenses, and Counterclaim (Doc # 20). Defendants’ Counterclaim seeks a Declaratory Judgment by this Court that the contractual limitation of liability provision relied on by Plaintiff does not apply in this case.

5. Pursuant to Rule 12(c) of the Federal Rules of Civil Procedure, Defendants now move for judgment on the pleadings on all claims in the Complaint and their Counterclaim. Judgment on the pleadings is properly granted where the moving party has clearly established that no material issue of fact remains to be resolved and the party is entitled to judgment as a matter of law. The proper interpretation of an unambiguous contract is an appropriate matter for a court to consider on such a motion.

6. The Complaint describes an inter-related series of written agreements among Schnucks, First Data, and Citicorp concerning the processing of credit and debit card transactions at Schnucks retail locations. (Complaint, Doc. #9, at ¶¶ 12, 16-17). These inter-related agreements are: (1) a Master Services Agreement (“MSA”) (Exhibit A hereto); (2) a Bankcard Addendum to the MSA (“Bankcard Addendum”) (Exhibit B hereto); and (3) Program

Terms and Conditions (“Operating Procedures”) (Exhibit C hereto).¹

7. In October 2011, Schnucks and First Data entered into the MSA. (Exhibit A). The MSA establishes “the terms and conditions by which First Data agreed to provide credit and debit card merchant transaction processing services for Schnucks.” (Complaint, Doc. #9, at ¶ 16).²

8. Section 5.4 of the MSA contains a limitation of liability provision:

“Limitation of Liability. NOTWITHSTANDING ANYTHING IN THIS MSA AND ANY ADDENDA TO THE CONTRARY, CUSTOMER, FDMS AND ITS AFFILIATES’ CUMULATIVE LIABILITY, IN THE AGGREGATE (INCLUSIVE OF ANY AND ALL CLAIMS MADE BY CUSTOMER, FDMS AND/OR ITS AFFILIATES, WHETHER RELATED OR UNRELATED) FOR ALL LOSSES, CLAIMS, SUITS CONTROVERSIES, BREACHES, OR DAMAGES FOR ANY CAUSE WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, THOSE ARISING OUT OF OR RELATED TO THIS MSA AND ANY ADDENDA) AND REGARDLESS OF THE FORM OR ACTION OR LEGAL THEORY SHALL NOT EXCEED \$500,000. NOTWITHSTANDING THE FOREGOING, CUSTOMER, FDMS AND ITS AFFILIATES’ CUMULATIVE LIABILITY FOR ITS BREACH UNDER SECTION 25 (DATA SECURITY) SHALL NOT EXCEED \$3,000,000. FOR PURPOSES OF CLARIFICATION, EITHER PARTY CUMULATIVE TOTAL UNDER THIS CONTRACT SHALL NOT EXCEED \$3,500,000. **THIS SECTION 5.4 LIMITATION OF LIABILITY SHALL NOT APPLY TO CUSTOMER’S LIABILITY FOR CHARGEBACKS, SERVICERS’ FEES, THIRD PARTY FEES, AND FEES, FINES OR [PENALTIES] BY THE ASSOCIATION OR ANY OTHER CARD OR DEBIT CARD PROVIDED UNDER THIS MSA OR ANY ADDENDA.**”

(Exhibit A at § 5.4 (emphasis added)).

¹ The MSA, the Bankcard Addendum, and the Operating Procedures are also attached (with certain agreed to redactions) to Defendants’ Answer and Counterclaim (Doc. #20) as Exhibits A, B, and C. The Court is free to consider these documents here because they are integral to the disposition of the Complaint.

² The MSA is controlled by Missouri law. (Exhibit A at § 11).

9. Contemporaneous with the signing of the MSA, Plaintiff and Defendants executed a Bankcard Addendum to the MSA. (Complaint, Doc. #9, at ¶¶ 16-17; Exhibit B hereto). The Bankcard Addendum incorporates the MSA and “sets forth the terms and conditions by which First Data *and Citicorp* collectively agreed to provide credit and debit card merchant transaction processing services for Schnucks.” (Complaint, Doc. #9, at ¶ 16 (emphasis added); Answer to Counterclaim, Doc. #30, at ¶ 6).

10. The Bankcard Addendum imposes all financial responsibility on Schnucks for invoices directed to Defendants by “Third Parties,” such as Visa and MasterCard (a/k/a the credit card Associations), arising out of a data security breach:

CUSTOMER [Schnucks] shall at all times be responsible for, payment for all fees and charges (including increases[,] additions, or modification made thereto), **without limitation, of any Credit Card Association [Visa and MasterCard],** Network, card-issuing organization, telecommunications provider, federal, state or local governmental authority (each a ‘Third Party’) **including, without limitation any switch fee, issuer, reimbursement fee, adjustment fee, interchange fee, assessment fee or access fee, (collectively, ‘Third Party Fees’).**

(Exhibit B at § 13.3 (emphasis added)). Further, Section 13.5 of the Bankcard Addendum memorializes Schnucks’ agreement to pay “any *fin*es, *fe*es, or *pen*alties” arising out of Plaintiff’s own “negligent acts or omissions.” (*Id.* at § 13.5 (emphasis added)).

11. The Bankcard Addendum also requires that Plaintiff implement a data security program, and thus be “PCI compliant” at all times,³ as defined by the Associations stating:

. . . CUSTOMER [Schnucks] is required to follow the Operating Procedures and comply with Association Rules as they may each be amended from time to time. The Association may impose different compliance requirements on different types and levels of customers. The Association may impose restrictions, fines, or prohibit CUSTOMER from participating in Association programs if it is

³ “PCI” stands for “payment card industry.”

determined CUSTOMER is non-compliant with such programs. **CUSTOMER understands that it must be in compliance with data security regulations for its type or level of customer as defined by the Associations security procedures as well as comply with general security procedures.**

(Exhibit B at § 25 (emphasis added)). In connection with these data security requirements, the Bankcard Addendum reiterates that “. . . CUSTOMER [Schnucks] understands and acknowledges that it is *solely the responsibility of CUSTOMER* to maintain compliance with all Association PCI Data Security procedures and regulations, and *to pay any and all fines levied by the applicable Association* for its non-compliance . . .” (*Id.* (emphasis added)).

12. The Bankcard Addendum incorporates the Program Terms and Conditions (or “Operating Procedures”) and the MSA incorporates the operating regulations of the Associations. (Exhibit B at § 4; Exhibit C hereto; Complaint, Doc. #9, at ¶ 17).⁴ Section 4.9 of the Operating Procedures details Schnucks’ data security obligations and *its financial responsibility* over to the Associations for failure to fulfill those obligations:

If you [Schnucks] or a Merchant Provider (or other Person used by you) are determined by any Card Organization, regardless of any forensic analysis or report, to be the likely source of any loss, disclosure, theft or compromise of Cardholder data or Card transaction information, or caused Cardholder data to be put at risk (together, ‘Compromised Data Events’) and regardless of your belief that you have complied with the Card Organization Rules or any other security precautions and are not responsible for the Compromised Data Event, **you must promptly pay us for all related expenses, claims, assessments, fines, losses, costs and penalties and Issuer reimbursements imposed by the Card Organizations against us** (together, ‘Data Compromise Losses’).

(Exhibit C at § 4.9 (emphasis added)).

⁴ It is undisputed that the MSA, Bankcard Addendum, and Operating Procedures constitute one entire, integrated contract between Plaintiff and Defendants. (Complaint, Doc. #9, at ¶¶ 16-17; Exhibit B (Bankcard Addendum) at § 26.3 (“*The Bankcard Addendum, along with the [MSA] . . . and the Operating Procedures, constitutes the entire agreement between the parties with respect to the subject matter*”) (emphasis added)).

13. To secure these financial obligations, the Bankcard Addendum permits Defendants to create and maintain a special reserve account (the “Reserve Account”) from Schnucks’ payment card transaction flow. (Complaint, Doc. #9, at ¶ 19; Exhibit B at § 22).

14. On March 30, 2013, Plaintiff experienced a cyber-attack against its payment card processing system that “involved the insertion of malicious computer code that searched for the presence of data from the magnetic stripe of payment cards swiped” at certain of Schnucks’ affected retail locations. (Complaint, Doc. #9, at ¶¶ 24-25). The Associations characterize such cyber-attacks as “data compromise events.” (*Id.* at ¶ 27).

15. If the Associations maintain that a merchant was not “PCI compliant” at the time of a data breach, they may assess a “non-compliance fine” and/or a “case management fee” against the acquiring bank (here, Citicorp). (Complaint, Doc. #9, at ¶ 27). Additionally, when the data compromise event involves data procured from payment card magnetic stripes, the Associations can issue assessments against the acquiring bank as reimbursement for: “(1) the amount that the [payment card] issuing banks spent to monitor or cancel and re-issue at risk cards; and (2) the amount of fraudulent charges on the at risk cards.” (*Id.*).

16. As a direct result of Schnucks’ data breach, “First Data received a preliminary case management report from MasterCard outlining the case management fee and the amount of monitoring/card replacement and fraud loss reimbursement it was assessing against Citicorp.” (Complaint, Doc. #9, at ¶ 28). Based on MasterCard’s assessment, First Data projected the total dollar amount of Visa’s anticipated assessment arising out of the breach. (*Id.* at ¶ 29). As expressly permitted by the MSA and Bankcard Addendum, First Data then established the Reserve Account for the Associations’ actual and projected assessments by “withholding a percentage each day from the funds First Data collected for Schnucks from the payment card

transactions [First Data] processed at one [Schnucks'] store location.” (*Id.* at ¶¶ 30-31). To date, Visa has yet to finalize its assessment for Schnucks’ data breach. (*Id.* at ¶¶ 29-30).

17. The dollar amount held in the Reserve Account to cover the Associations’ fees, fines, and assessments well exceeds \$500,000. (Complaint, Doc. #9, at ¶ 33).

18. Under Missouri law, unambiguous contracts are enforced according to their plain language. A determination of whether a contractual provision is ambiguous is a question of law for the Court.

19. Defendants are entitled to judgment on the pleadings because the plain and unambiguous language of the MSA and its incorporated agreements, together with the admissions in Plaintiff’s Complaint (Doc # 9) and Answer to Defendants’ Counterclaim (Doc # 30), establish that Plaintiff is liable for *all* of the financial responsibility imposed on Defendants by the Associations relating to the cyber-attack on Schnucks’ payment card processing system and the resulting data security breach.

20. Given that Plaintiff is indisputably liable for all expenses and assessments in connection with Schnucks’ data security breach, Defendants properly exercised their rights under the Bankcard Addendum and Operation Procedures to establish the Reserve Account at a sum sufficient to cover the Associations’ assessments against Defendants. Thus, the only remaining dispositive issue in this case is whether the dollar amount of Plaintiff’s admitted financial responsibility is subject to a limitation in the parties’ agreements.

21. While Schnucks acknowledges its liability for the financial responsibility being assessed against Defendants by Visa and MasterCard, it tortures the MSA’s language to conclusorily assert that this liability is limited to the \$500,000 figure mentioned in Section 5.4 of the MSA.

22. Plaintiff's erroneous interpretation ignores the express language of Section 5.4 of the MSA that unambiguously sets forth an exception to that limitation on liability for: (1) Third Party Fees charged by Visa or MasterCard to Defendants as a result of a data compromise event, including fees related to fraud reimbursement and recovery; and/or (2) fees (including reimbursements and assessments), fines or penalties charged by Visa or MasterCard based on Schnucks' failure to comply with the applicable Payment Card Industry Data Security (PCIDSS) requirements (*i.e.*, for not being "PCI compliant").

23. The Complaint admits that the Reserve Account is exclusively comprised of funds recouped by Defendants from Plaintiff's payment card transaction flow in order to cover Third Party Fees assessed by the Associations arising out of Plaintiff's data breach.

24. Defendants therefore properly recovered from Plaintiff, through the Reserve Account, the actual and potential financial liability arising out of Schnucks' data breach in the full amount of their combined actual and potential liability to the Associations.

25. Defendants respectfully submit a Memorandum in Support of its Motion for Judgment on the Pleadings, which it adopts and incorporates by reference.

WHEREFORE, for all of the aforementioned reasons, as well as those set forth in the accompanying Memorandum, Defendants/Counterclaim-Plaintiffs First Data Merchant Services Corp. and Citicorp Payment Services, Inc. respectfully request that this Honorable Court grant their Motion for Judgment on the Pleadings.

Respectfully Submitted,

FOX ROTHSCHILD LLP

Dated: May 19, 2014

By: /s/ Joshua Horn
Joshua Horn (admitted *pro hac vice*)
Amy C. Purcell (admitted *pro hac vice*)
FOX ROTHSCHILD LLP
2000 Market Street, 10th Floor
Philadelphia, PA 19103
215-299-2000
Fax: 215-299-2150
Email: jhorn@foxrothschild.com
Email: apurcell@foxrothschild.com

ATTORNEYS FOR DEFENDANTS AND
COUNTERCLAIM PLAINTIFFS FIRST DATA
MERCHANT SERVICES CORP. AND CITICORP
PAYMENT SERVICES, INC.

Lucy T. Unger, #36848
Patrick I. Chavez, #47732MO
Bank of America Tower
100 North Broadway, 21st Floor
St. Louis, Missouri 63102
314/345-5000
314/345-5055 (FAX)
lunger@wvslaw.com
pchavez@wvslaw.com

Nicholas T. Solosky (admitted *pro hac vice*)
FOX ROTHSCHILD LLP
1030 15th Street, N.W.
Suite 380 East
Washington, DC 20005
202-461-3100
Fax: 202-461-3102
Email: nsolosky@foxrothschild.com